UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

18 MAG 9733

In the Matter of a Warrant for All Content and Other Information Associated with the Google Accounts pthimot@gmail.com, imaginehealthinc@gmail.com, emergentfl@gmail.com, Maintained at Premises controlled by Google LLC, USAO Reference No. 2018R01109

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

MICHAEL RYAN, Special Agent with the Federal Bureau of Investigation, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately 16 years. I am currently assigned to a cyber intrusion squad at FBI's New York Field Office. I have participated in investigations into criminal offenses involving computer and wire fraud, and am familiar with the means and methods used to commit such offenses. In that capacity, I have received training in the review of electronic evidence and have participated in the execution of search warrants involving electronic evidence.

B. The Provider, the Subject Account and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the Google accounts pthimot@gmail.com (**"TARGET GOOGLE ACCOUNT-1"**), imaginehealthinc@gmail.com

("TARGET GOOGLE ACCOUNT-2"), emergentfl@gmail.com **("TARGET GOOGLE ACCOUNT-3")**, maintained and controlled by Google LLC ("Google" or the "Provider") headquartered at 1600 Amphitheatre Parkway, Mountain View, CA. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer fraud and abuse), 1343 (wire fraud), 1344 (bank fraud), 1956 (money laundering) and 2315 (receipt of stolen goods) (the "Subject Offenses"). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email and electronic data storage sites in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

4. I have learned the following about the Provider:

a. The Provider offers email services to the public. In particular, the Provider allows subscribers to maintain email accounts under any domain name under the subscriber's control. For example, if a subscriber controls the domain name "xyzbusiness.com," the Provider enables the subscriber to host any email address under this domain name (*e.g.*, "john@xyzbusiness.com"), on servers operated by the Provider. A subscriber using the Provider's services can access his or her email account from any computer connected to the Internet.

b. The Provider maintains the following records and information with respect to every subscriber account:

i. *Email contents*. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Provider's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Provider's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for a certain period of time.

ii. *Address book.* The Provider also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* The Provider collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Provider also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the Provider maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Device Information.* The Email Providers collect and maintain information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity

Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

v. *Cookie Data.* The Provider uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at the provider using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by the Provider when a computer visits its site or logs into an account.

vi. *Transactional information.* The Provider also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider's website).

vii. *Customer correspondence.* The Provider also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

viii. *Preserved and backup records.* The Provider also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). The Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

c. In addition, the Provider also maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

i. *Google Drive content*. Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

ii. *Google Docs*. Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive.

iii. *Google Photos*. Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable

image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

iv. *Google Calendar*. Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

v. *Google Chats and Google Hangouts content*. Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's email and chat content.

vi. *Location History data*. Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

vii. *Google Payments*. Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

viii. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at http://www.google.com, and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

D. Jurisdiction and Authority to Issue Warrant

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

Criminal Activity and Use of Email by NANCY MARTINO-JEAN

8. On or about September 15, 2018, NANCY MARTINO-JEAN was charged in Complaint 18 Mag. 8070 (the "Complaint") filed in the Southern District of New York with wire

fraud, in violation of Title 18, United States Code, Section 1343 and receipt of stolen funds, in violation of Title 18, United States Code, 2315. The Complaint is attached hereto as Exhibit A and is incorporated by reference herein.

9. On the day of her arrest, and the following day, MARTINO-JEAN, after having been informed of her *Miranda* rights and waiving those rights, made the following statements to law enforcement, set forth here in substance and in part:

a. The $1.7 million wire transfer was a loan, MARTINO-JEAN believed, from Company-1.[1]

b. MARTINO-JEAN sent information regarding her real estate projects to what she believed was Company-1 via her personal email account (the "Martino-Jean Google Account") and an email account associated with one of her businesses.

c. MARTINO-JEAN executed a contract with Company-1 via email that provided for a $1.7 million loan to MARTINO-JEAN at an 18% annual interest rate. MARTINO-JEAN was to begin paying her loan payments in January 2019.

d. MARTINO-JEAN recalled primarily communicating with a Company-1 representative with the first name "Raji."

2. On or about September 28, 2018, the Honorable Stewart D. Aaron signed a warrant authorizing the search of the contents of the Martino-Jean Google Account.

[1] For a number of reasons, including that MARTINO-JEAN previously told the person identified in the Complaint as "Individual-1" that the source of the funds was an inheritance from her mother in Haiti, I do not credit her claim that she believed the funds were a legitimate loan from Company-1.

Evidence of Criminal Activity Uncovered in the Martino-Jean Google Account

4. Based on my review of the Google search history associated with the Martino-Jean Google Account, I have learned the following, in substance and in part:

a. On or about August 12, 2018, MARTINO-JEAN searched for "[Company-1]." Based on the information provided by Google, this was the first and only search by MARTINO-JEAN which contained the name of Company-1.

b. On or about August 13, 2018, MARTINO-JEAN searched for "how to write out a window computer," "how to write out a computer," and "how to remove everything from a computer." In addition, on that same day, MARTINO-JEAN visited a webpage entitled "How to erase my hard drive and start over," which contained detailed instructions on how to erase all of the information on a hard drive. On that same day, MARTINO-JEAN also searched for "[common abbreviation of Bank-1] fraud department."

5. Based on my review of the contents of the email account associated with the Martino-Jean Google Account, I have learned the following, in substance and in part:

6. On or about August 14, 2018 at 10:08 a.m., **TARGET GOOGLE ACCOUNT-1** (which displays the name "pierre thimot" next to the email address) sent an email ("Email-1") to **TARGET GOOGLE ACCOUNT-3** (which displays the name "Mustafa Line" next to the email address), which contained the text "THANK YOU!" and attached seven PDF documents entitled "Scan 1" through "Scan 7" (collectively, the "Scanned PDF Files"). The Scanned PDF Files are attached hereto as Exhibit B. The subject heading of Email-1 is "SECURITY AGREEMENT." Each of the Scanned PDF Files is one-page.

7. On or about August 16, 2018 at 9:04 a.m., **TARGET GOOGLE ACCOUNT-1** forwarded Email-1 to the MARTINO-JEAN Google Account.

8. Scan 1 is entitled "Security Agreement and Promissory Note." It purports to be a Security Agreement "made and effective 07/02/2018" between Company-1 and the company identified as "Company-2" in the Complaint. Based on my review of publicly available records from the Florida Secretary of State, I know that MARTINO-JEAN is the President and Registered Agent of Company-2 and the Vice-President of Company-2 is an individual named "Mustapha Raji." Scan 1 states that the head office of Company-1 is located in Hong Kong. I know, based on my participation in this investigation, that the headquarters of Company-1 are located in Manhattan, New York. Scan 1 further provides that Company-2 will pay Company-1 $1.7 million at an annual interest of 12% and that repayment shall begin on January 15, 2019 and be paid in monthly installments of $204,000.[2]

9. Scan 5 includes a signature block for the "debtor" and the "secured party." However, the names of the debtor and the secured party are not identified.

10. Scan 6 also appears to be the signature page of a document. At the top of the page in capital letters, text reads, "We understand that we are swearing or affirming under oath to the truthfulness of the claim made in this affidavit and that the punishment for knowingly making a false statement includes fines and/or imprisonment."[3] There are then two lines which appear to be signature lines. Next on the page are the words "Notary Page," the state and county, and the words "Sworn to or affirmed and signed before me on this [blank line] day of [blank line] 2018

[2] Based on my review of public court filings, I have learned that on or about February 14, 2018, Company-2—the company purportedly receiving a $1.7 million "loan"— filed for Chapter 11 bankruptcy in the U.S. Bankruptcy Court for the Southern District of Florida. On or about April 12, 2018, the bankruptcy court granted a motion by the U.S. Trustee to dismiss Company-2's case with prejudice, because Company-2 had failed to provide the U.S. Trustee with requested documents, including proof of insurance.

[3] This same text is repeated at the bottom of the page.

by [blank line]." There is also a blank signature line for a "Notary Public." Scan 6 contains no signatures.

11. On or about August 15, 2018 at 9:09 p.m., **TARGET GOOGLE ACCOUNT-2** sent an email ("Email-2") to **TARGET GOOGLE ACCOUNT-1** with a PDF attachment entitled "port" ("PDF-2"). About two minutes later, **TARGET GOOGLE ACCOUNT-1** forwarded Email-2 to the Martino-Jean Google Account. There is no text in the body of either email.

12. PDF-2 is one-page and appears to be a partially-completed version of Scan 6. It is attached hereto as Exhibit C. At the top of the page in capital letters, text reads, "We understand that we are swearing or affirming under oath to the truthfulness of the claim made in this affidavit and that the punishment for knowingly making a false statement includes fines and/or imprisonment."[4] There are then two lines which appear to be signature lines. Next on the page are the words "Notary Page," the state and county, and the words "Sworn to or affirmed and signed before me on this 02 day of July, 2018 by [blank line]." The "02" and "July" in that sentence are handwritten. The document then appears to bear the notary stamp of a particular notary and that notary's signature. Based on my training and experience, I know that a notarization typically reflects that an individual or individuals—whose identities have been verified by a notary—have signed a document in the presence of that notary. However, there are no signatures anywhere on PDF-2, nor are there any printed names under the signature lines.

13. Based on my training and experience, and my participation in this investigation, I believe that the purported "Security Agreement" contained in the Scanned PDF Files and PDF-2 is a fraudulent document created to conceal the criminal activity described in the Complaint and that the users of the Subject Accounts participated in its creation and/or dissemination.

[4] This same text is repeated at the bottom of the page.

10. Based on the foregoing, I submit that there is probable cause to believe that the Subject Accounts were an instrumentalities of, and contain evidence of, the Subject Offenses, including evidence concerning the identity of the user of the Subject Accounts. This Application seeks authority to search these accounts from November 1, 2017 through the present.

11. The Subject Accounts' activity, logs, stored electronic communications, and other data retained by the Providers for the accounts can indicate who has used or controlled the accounts, as discussed in more detail in paragraph 10.

12. In my training and experience, evidence of who was using an email account may be found by viewing emails written or received during the relevant time period, and attachments to those emails, including pictures and files, address books, and contact or buddy lists. Accordingly, a review of the entire content of the Subject Accounts during the relevant time period may be necessary to ascertain the identities of the individuals that used the Subject Account contemporaneously with the time at which the Subject Accounts was used in furtherance of the Subject Offenses.

13. In addition, the Subject Accounts may contain information that will confirm the identities of any co-conspirators and other victims and otherwise relevant communications that relate to topics concerning the Subject Offenses, including victim selection and targeting, and the receipt and transfer of stolen funds.

A. Evidence, Fruits and Instrumentalities

14. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

15. In particular, I believe the Subject Accounts are likely to contain the following information:

a. Information identifying or the location of the user of the Subject Accounts, and the individual involved in the Subject Offenses, including photographs or videos depicting the user of the Subject Accounts, communications with individuals that the user of the Subject Accounts trusts, which reveal his identity or include information that can be used to ascertain his identity, such as travel information or receipts for online purchases or other communications with social network websites or third party service providers;

b. Communications or documents created to conceal the Subject Offenses or the identities of the participants involved in the Subject Offenses;

c. Communications with the user of the Subject Accounts with other co-conspirators and other subjects about the Subject Offenses, including but not limited to obtaining unauthorized access to and data from computer systems, reconnaissance of victim computer systems, victim selection and targeting, malicious software, software vulnerabilities, malicious domains, spearphishing emails, exfiltrating system data, creation of fraudulent personas, trafficking in stolen credit card numbers, and monetizing stolen personal and computer system information belonging to other individuals, and communications and other data identifying such co-conspirators;

d. Fake identification documents;

e. Documents, spreadsheets and ledgers tracking spearphishing and computer hacking attacks;

f. Spearphishing emails, seeking to induce victims to click on hyperlinks, download attachments, or otherwise take action to infect victim systems with malware, and test versions of the same;

g. Copies of malicious software, keyloggers, email crackers, email scrapers, or other malware used to obtain unauthorized access to computer systems, and communications with others regarding such tools, or obtaining and trafficking in them;

h. Information stolen from computer systems through unauthorized access and computer intrusion;

i. Communications regarding the purchase, sale, monetization or transfer of personal and other information stolen through computer intrusions;

j. Evidence concerning the user's technical expertise;

k. Information regarding the registration of other email accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, and payment for such online facilities or services; and

l. Evidence concerning any other online accounts or any computer devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

III. Review of the Information Obtained Pursuant to the Warrant

16. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement

personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

17. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

18. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert

potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. As set forth above, the target(s) of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. Indeed, the target(s) have already attempted to delete evidence relating to this investigation. The Government is informed by a representative of Company-1 that certain of the email communications received by Employee-2 had been deleted, but were later recovered. *See* 18 U.S.C. § 2705(b)(3). Additionally, the target(s) appear to have the financial means that would facilitate their flight from prosecution. *See* 18 U.S.C. § 2705(b)(2).

19. Accordingly, there is reason to believe that, were the Provider to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

20. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V.Conclusion

21. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C.

§ 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

Michael Ryan
Special Agent, FBI

Sworn to before me this
_____ day of November, 2018

NOV 15 2018

S/Barbara Moses

THE HONORABLE BARBARA C. MOSES
UNITED STATES MAGISTRATE JUDGE
Southern District of New York